

5.8 Az EGSZB fenntartja azt az álláspontját, amely szerint a 4056/86 rendeletet hatályon kívül kellene helyezni, és az Európai Bizottság új, a vonalhajózási konferenciáról szóló – csoportmentességet biztosító – rendeletével kellene pótolni. Az új rendszernek szigorúan igazodnia kellene az Elsőfokú Bíróság és az Európai Bizottság hatáskörében kialakított kritériumokhoz (pl.:TACA ügy). A konferenciarendszert az uniós hajótulajdonosok egész világra kiterjedő versenyképességének megőrzése érdekében is fenn kellene tartani. Míg a nagy szállítótársaságok számára megfelelőek lehetnek a „szövetségek” és egyéb együttműködési formák, a kis és közepes szállítótársaságok számára piaci részesedésük megőrzése érdekében továbbra is szükség van a konferenciákra, különösen a fejlődő országokkal folytatott kereskedelemben. A mentesség megszüntetése versenyellenes hatásokkal járhatna e kis szállítótársaságokra, és erősítené a nagyobbak erőfölényét.

5.9 Az Európai Bizottságnak arra kellene fordítania az átmeneti időszakot, hogy figyelemmel kíséri a piaci fejleményeket, beleértve az egyesülési tendenciákat. Az Európai Bizottságnak

ezenkívül konzultációkat kellene kezdenie egyéb joghatóságokkal (OECD) annak érdekében, hogy más, a jogrendszerekkel világszerte összeegyeztethető, megfelelő rendszerben állapodjanak meg.

5.10 Az EGSZB támogatja a Fehér Könyv trumphajózási szolgáltatások és kobotázis-szolgáltatások kezelésére vonatkozó javaslatát, mivel ezekben az ágazatokban az esetek nagy részében nem merülnének fel versenyproblémák. A jogbiztonság érdekében azonban az EGSZB arra kéri az Európai Bizottságot, hogy nyújtson jogi útmutatásokat az ömlesztett áruk pooljának és a szakosított kereskedelmi tevékenységeknek az önbecsléséről abban a tekintetben, hogy összeegyeztethető-e az EK-Szerződés 81. cikkével.

5.11 Az EGSZB kifejezi azon reményét, hogy segítséget nyújthat a Fehér Könyv által megindított gondolkodási folyamat továbbvitelében.

Brüsszel, 2004. december 16.

Az Európai Gazdasági és Szociális Bizottság
Elnöke
Anne-Marie SIGMUND

Az Európai Gazdasági és Szociális Bizottság véleménye a „Javaslat európai parlamenti és tanácsi határozatra az internet és az új on-line technológiák biztonságosabb használatának előmozdítását célzó többéves közösségi program létrehozásáról”

COM(2004) 91 végleges – 2004/0023 (COD)

(2005/C 157/24)

2004. március 26-án a Tanács úgy határozott, hogy az Európai Közösséget létrehozó Szerződés 153. cikke alapján kikéri az Európai Gazdasági és Szociális Bizottság véleményét a fent említett témában.

Az ide vonatkozó bizottsági munkákkal megbízott „Közlekedés, energia, infrastruktúra és információs társadalom” szekció 2004. október 5-én elkészítette véleményét (előadó: Daniel RETUREAU, társelőadó: Ann DAVISON).

2004. december 15-én és 16-án megtartott 413. plenáris ülésén (2004. december 16-i ülés), 147 igen szavazattal és 1 tartózkodás mellett az EGSZB elfogadta a következő véleményt:

1. A véleménytervezet összefoglalása

1.1 Az Európai Bizottság új, ám az információs társadalomban a távközlési hálózatok terén lezajlott gyors fejlődésre való tekintettel a korábbi programhoz képest megerősített „Safer Internet” projekt elindítását javasolja. Ezért kapta a program a „Safer Internet plus” (2005–2008) nevet.

1.2 Az Európai Bizottság parlamenti és tanácsi határozatra vonatkozó javaslatán kívül az EGSZB megvizsgálta a „Safer Internet plus” (2005–2008) programnak egy bizottsági munkadokumentumban (SEC(2004) 148) és a „COM(2004) 91 végleges” jelzésű dokumentumban található előzetes értékelését

is. Az EGSZB támogatja az új akcióterv alkalmazási körének kiterjesztését és az abban foglalt új célkitűzéseket, melyek számításba veszik az on-line hozzáférés gyors és szerteágazó fejlődését, valamint a szélessávú átvitelre alkalmas hozzáférések és az állandó hálózati kapcsolatok számának ugrásszerű emelkedését. Ehhez az általános és a külön megjegyzésekben politikai és szabályozási intézkedésekre vonatkozó kiegészítő javaslatokat fűz, mégpedig a következő területeken:

- a (kötelező és önkéntes) technikai és jogi szabványok ill. normák;
- a felhasználók képzése és oktatása;

- a tárhely- és hozzáférés-szolgáltatók és más szereplők kötelezettségei (hitelkártya-társaságok, keresőprogramok...);
- a szoftverkészítők és a biztonsági szolgáltatók felelőssége;
- a sebezhető személyek védelme a csalások vagy kétes információk ellenében (különböző szélhámosságok, aktív gyógyszerek „szabad” árusítása, orvosi képzéssel nem rendelkező személyek által nyújtott egészségügyi tanácsadás vagy kezelés...).

2. Az Európai Bizottság javaslatai (összegzés)

2.1 A javasolt program az Internet és az on-line technológiák biztonságosabb használatát kívánja előmozdítani a végfelhasználók, különösen a gyerekek és a fiatalok számára, otthon és az iskolában egyaránt. Ebből a célból a tervekben szerepel olyan, egyesületek és más csoportosulások (kutatócsoportok, programkészítők, oktatási intézmények...) által készített projektek társfinanszírozása, amelyek védelmi eszközök – „forró segélykérő vonalak”, levélszemét és vírus elleni programok, „intelligens” keresők stb. – kifejlesztésére irányulnak.

2.2 A biztonságosabb Internetet célzó korábbi akciótervet (1999–2002) 2003–2004-re meghosszabbították.

2.3 Az Európai Bizottság honlapja felsorolja a *Safer Internet* (Biztonságosabb Internet) program keretében 2003 végéig megvalósult projekteket⁽¹⁾.

2.4 A jelenlegi javaslat (2005–2008) kiterjed az új on-line kommunikációs eszközökre is, melyek esetében igyekszik határozottabban fellépni a jogtalan és káros tartalmakkal szemben, beleértve ebbe a vírusokat és az egyéb károkozásra alkalmas vagy nem kért (*spam*) tartalmakat.

2.5 Az európai intézmények szemszögéből ezt a határozottabb fellépést több szempont is indokolta teszi, melyek közül a legfontosabbak a következők:

- a szélessávú, hosszú időtartamú vagy állandó Internet hozzáférés gyors terjedése a magánszemélyek, a vállalatok, a közigazgatás és a magánszféra intézményei (civil szervezetek) körében;
- az Internet hozzáférés, valamint az új, gyakran nem kért online tartalmakhoz (*e-mailek*, *SMS-ek*) és a vonzóbb tartalmakhoz (multimédia) való hozzáférés eszközeinek és módszereinek szerteágazó fejlődése;
- a nem kívánt és potenciálisan veszélyes vagy nem helyénvaló tartalmak drámai mértékű terjedése új veszélyeket teremt általában a felhasználók számára (vírusok: tárhelyek elárasztása, adatok eltérítése vagy megsemmisítése, az áldozat kommunikációs eszközeinek felhatalmazás nélküli használata; *spamek*: sávszélességgel és tárhellyel kapcsolatos visszaélés, elektronikus levélszekrények elárasztása, ami megbénítja vagy zavarja az Internet hozzáférést és a kommu-

nikációt, valamint olyan jelentős költségeket okoz, melyeket nem a „szennyező”, hanem a végfelhasználó kell, hogy viseljen) és szűkebb értelemben bizonyos felhasználói csoportok, így a gyermekek számára (explicit szexuális tartalommal bíró *spamek*, nem helyénvaló üzenetek és találgatások pedofilek részéről a csevegő-fórumokon (*chat room-okban*));

- gyermekek számára könnyen hozzáférhető nem helyénvaló tartalmak, melyek kiszűrése a gyermekekért felelősséget viselő személyek rendelkezésére álló eszközök igencsak viszonylagos hatékonysága miatt nehézségekbe ütközik.

2.6 A program fő célja a gyermekek védelme és azok támogatása, akik felelősséget viselnek értük (szülők, tanárok, oktatók stb.) vagy erkölcsi érdekeik és jólétük védelmében fellépnek. Ebben az értelemben a program érinti mindazokat a civil szervezeteket, amelyek a szociális szektor, a gyermekjogok, a rasszizmus, az idegengyűlölet (?) és a diszkrimináció minden egyéb formája elleni fellépés, a fogyasztóvédelem és a polgári szabadságjogok védelme területén vagy ezekkel rokon területeken tevékenykednek.

2.7 Érinti ezenkívül a kormányokat, a törvényhozó, igazságügyi és rendőri szervezetet, valamint a szabályozó hatóságokat. Mind az anyagi jogot, mind az eljárásjogot hozzá kell igazítani ezekhez a követelményekhez és kellő számú embert kell kiképezni és ellátni a megfelelő eszközökkel.

2.8 A program jelentőséggel bír az ágazat számára is, melynek biztonságos környezetre van szüksége, hogy megerősítse a fogyasztók bizalmát.

2.9 Az egyetemek és kutatóintézetek tisztázhatják a gyermekek új médiahasználati szokásait. A biztonsággal kapcsolatos üzenetek eljuttatásának legjobb módja az ilyen médiákkal kapcsolatos büntetőeljárások megismertetése, az új technikai megoldások keresése és egy független álláspont kialakítása a szabályozási eljárások és az önszabályozás érdekeinek összeegyeztetésével kapcsolatban.

2.10 A program két tevékenységi körre terjed ki: Társadalmi szinten azokra a területekre koncentrál, ahol a szabályozás és a piac önmagukban képtelenek lennének a felhasználók biztonságának biztosítására. Gazdasági szinten a cél az Internet és az on-line technológiák biztonságos használatának előmozdítása a bizalom légkörének megteremtése révén.

2.11 Mintegy 50 millió eurós keret áll majd a tervek szerint rendelkezésre technikai és jogi eszközök, szoftverek és tájékoztató anyagok létrehozására annak érdekében, hogy sikeresebben lehessen felvenni a harcot a hálózatokat és a végpontokat érő támadásokkal, valamint az azokkal való, nem kívánt és esetenként erkölcsi, társadalmi vagy gazdasági kárt okozó tartalmak révén történő visszaélésekkel szemben.

⁽¹⁾ http://www.europa.eu.int/information_society/programmes/iap/index_en.htm

⁽²⁾ Ezek a témák már megjelentek az EGSZB egyik korábbi vizsgálatában.

3. Az EGSZB általános megjegyzései

3.1 Az EGSZB hivatkozik korábbi, a gyermekek internetes védelmére és az első akciótervre álláspontjára⁽¹⁾. Üdvözlí a világhálón terjesztett törvényellenes vagy kárt okozó tartalmak elleni új akciótervre tett javaslatot (lásd az 1. sz. összefoglalót a dokumentum elején). Támogatja a Safer Internet-plus program céljait és prioritásait, és a programot az egyik olyan eszköznek tekinti, amely az Internet biztonságának fokozását szolgálja. Mindazonáltal az EGSZB hangsúlyozza a probléma rendkívüli összetettségét és a nemzetközi fellépés, valamint a szabályozás szükségszerűségét a kérdéssel való eredményes szembenézés érdekében.

3.2 Az Internet és az on-line kommunikáció új technológiai (például a mobiltelefonok és a multimédia-funkcióval bíró, hálózatra csatlakoztatható PDA-készülékek, melyek komoly piaci sikereket érnek el) az EGSZB szemében a tudásalapú gazdaság, az e-gazdaság és az e-közigazgatás fejlődésének alapvető eszközei. Ezek a kommunikáció, a munka a kultúra és a szórakozás sokrétű eszközei. Ezért alapvető, hogy biztosítsuk a kommunikációs hálózatok működésének biztonságát és folyamatoságát, mivel olyan létfontosságú közszolgáltatásról van szó, amely nyitott és elérhető kell, hogy maradjon, és amelyben minden felhasználó meg kell, hogy tudjon bízni ahhoz, hogy a legjobb feltételek mellett használhassa ki az általa nyújtott ki sokféle lehetőséget. A biztonságosabb Internet használatával kapcsolatos tájékoztatás beépítése a különböző, így különösen az oktatási e-Európa programokba költséghatékonyasági szempontból az egyik legígéretesebb eszköz lenne jelentős számú ember elérésére.

3.3 Az Interneten uralkodó szólásszabadságnak és kommunikációs szabadságnak kedveznek a világhálóra kapcsolódás viszonylag alacsony költségei. Ez a nagysebességű átvitelre is igaz, amely egyre könnyebb hozzáférést biztosít a multimédiás tartalmakhoz. Csak néhány komoly demokratikus deficittel rendelkező ország igyekszik – a szabadságjogok folyamatos megsértése árán – állampolgárai kommunikációját és a számukra hozzáférhető tartalmakat ellenőrizni. Az EGSZB úgy ítéli meg, hogy nagyobb biztonságot kell garantálni, miközben megőrizzük és előmozdítjuk a tájékoztatási és kommunikációs, valamint a szólásszabadságot.

3.4 Azonban a világhálót, a kifejezés és az információ-áramlás szabadságának ezt a terét felhasználják – más kommunikációs eszközöknél még nagyobb mértékben – olyan illegális tevékenységekre, mint a pedofília vagy a rasszista és idegengyűlölő tartalmak terjesztése; bizonyos tartalmak pedig a közönség egy része, így különösen a fiatalok számára bizonyulhatnak károsnak, mint például a pornográfia vagy a házárdrjátékok (ez utóbbiak néhány országban be is vannak tiltva), valamint különböző bűncselekmények (sávszélességgel vagy adatokkal, illetve kiszolgálókkal való visszaélések). Az EGSZB tehát helyesli az akcióterv kiterjesztését az elektronikus

kommunikáció mindazon eszközeire, amelyekhez külső személy nem kívánt módon vagy ellenséges szándékkal hozzáférhet.

3.5 E dinamikus növekedést felmutató terület szabályozását bonyolítja az a jellegzetessége, hogy nyitott, és mindenki számára gyakorlatilag bármely ország bármely kiszolgálójáról vagy szabadon csatlakoztatott termináljáról elérhető. De sok országban még hiányoznak vagy elégtelenek az erre vonatkozó jogszabályok, ami lehetővé teszi, hogy az uniós Európában betiltott webhelyek tevékenységüket folytassák. Nagyon fontosnak tűnik, hogy az európai unió szóban és tettben nemzetközi fellépés mellett álljon ki – nevezetesen azokkal az észak-amerikai és ázsiai országokkal együttműködve, amelyekben nagyon elterjedt a szélessávú Internet hozzáférés –, hogy megvédjük a legkiszolgáltatottabbakat, és hogy hatékonyabban vehessük fel a harcot a *spam* ellen, mely az e-mailben történő kommunikáció fejlődését fenyegeti, csakúgy, mint a vírusok terjesztése ellen, amely sebezhetővé teszi a digitális gazdaságot. Bármennyire szükséges is a felhasználandó eszközök bevetése az európai uniós térségben, ezek egy globális megközelítés részeivé kell, hogy váljanak.

3.6 Mivel nincsenek nemzetközi egyezmények, bizonyos tartalmak bizonyos országokban való betiltása még a Világkereskedelmi Szervezethez benyújtott panaszhoz is vezethet a kereskedelem technikai akadályairól (TBT)⁽²⁾ szóló megállapodás értelmében, ezért erre a kérdésre ki kellene térni a folyamatban lévő tárgyalások során.

3.7 A jog területi hatálya és a nemzeti jogszabályok sokszínűsége nehezen megoldható problémát jelent. A technológiai szint lehetővé teszi az egyes emberek közötti mindenféle közvetlen fájlcsere (P2P, peer to peer), így ellenőrizhetetlen tartalmú rejtjeles fájlok cseréjét is. Minden, világhálóra csatlakoztatott gépet vagy hálózatot fel lehet használni egyre bonyolultabb tartalmak tárolására és küldésére, anonim és kinyomozhatatlan módon lehet csatlakozni bármely kiszolgálóhoz, mindezt nagyon fejlett, akár „feltörhetetlen” kódolási eljárások felhasználásával.

3.8 A személyes weblapok és weblogok divatja, a kereskedelmi webhelyek és az elektronikus pénzügyi szolgáltatások fejlődése, a tájékoztatási, oktatási, tudományos és technikai célú, de egyben a pornográf, házárdrjátékok csábító és egyéb honlapok sokasága azt eredményezi, hogy a világban több százmillió webhely létezik. Bizonyos fokú ellenőrzést lehetővé tesz a keresők általi kulcsszó-indexálás. Az Internet-szolgáltatók ellenőrizhetik a közvetlen kapcsolatot létrehozó és a tartalmakat (pl. *spam*-eket) automatikusan küldő webhelyeket. A nem kívánt reklámok és egyéb tartalmak lehetnek ugyanis általában véve károsak (sávszélesség telítése, vírusok terjesztése), vagy speciális problémákat okozhatnak bizonyos célközönségnek, pl. gyerekeknek (erkölcsi és pszichológiai értelemben vett károk).

⁽¹⁾ EGSZB-velemény a „Program a gyermekek védelme érdekében” címmel, előadó: DAVISON asszony, HL. C 48, 2002.2.21., valamint „Az Európai Bizottság közleményéről a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – A hálózatok és az információ biztonsága: javaslat európai szintű politikai megoldásra”, előadó: RETUREAU, HL C 48, 2002. 2. 21. és „A kiskorúak és az emberi méltóság védelméről az audovizuális és információs szolgáltatásokban” címmel, előadó: BARROW asszony, HL. C 1997. 9. 22.

⁽²⁾ „Technical Barriers to Trade”. Megállapodások a kereskedelem és a szolgáltatásnyújtás technikai akadályairól. Lásd pl. az USA vs. Antigua és Barbuda esetet az offshore pénzjátékok területén, a határozatot megfellebbezték a WTO-nál (http://www.wto.org/french/tratop_f/dispu_f/database_wto_members1_f.htm), dokumentum: 03-4429, WT/DS285/3 jelzéssel (2003.8.26.9.). Az ügy folyamatban.

3.9 Az Internet felhasználói között vannak maffiacsoportok, csalók, számítógépes vírusok szerzői, számítógépes kalózok, ipari kémek és más bűnözők, akik itt fejtik ki tevékenységüket. A bűnüldözés e területen nehéz helyzetben van, bár különleges rendőri egységek több országban is próbálják e csoportokat beazonosítani és tetten érni, hogy azután eljárhassanak ellenük és véget vethessenek a megállapított bűnös tevékenységeknek. Ez általában csak nemzetközi együttműködés révén lehetséges, amit ezért határozottabban elő kellene segíteni.

3.10 Hogyan harcoljunk az olyan bűnös tevékenységek, mint például a pedofil webhelyek ellen? Jogi szempontból a betiltásuk nem okoz problémát, de meg kell teremteni az ilyen hálózatok felgöngyölítésének eszközeit. Hogyan védjük meg a gyerekeket a pedofilektől, akik a fiatalok által különösen kedvelt csevegő fórumokon próbálnak találkákat megszervezni? A vita nem a tiltás és a bűnüldözés jogosságáról folyik ezekben a konkrét esetekben, hanem az ezek végrehajtásához szükséges eszközökről.

3.11 Az Internet-szolgáltatók nem felügyelhetik és ellenőrizhetik az összes náluk bejegyzett webhelyet és üzenetet (amelyek magánlevelezésnek minősülnek). Azonban bíró, rendőri vagy felhatalmazott gyermekvédelmi szerv megkeresésére az Internet-szolgáltatók kötelesek azonnal eleget tenni a hatóság webhely bezárására és felhasználóinak azonosítására vonatkozó felszólításának vagy határozatának. Ez azt jelenti, hogy a hálózati feltöltésekről és a kapcsolatokról szerzett információkat egy ideig tárolni kell.

3.12 Azonban a hitelkártya-társaságok, a keresőprogramok és az internetes szolgáltatók például időnként ellenőrzést végezhetnének – kulcsszavak és földrajzi zónák szerint – abból a célból, hogy felderítsék a pedofil vagy más bűnös tartalmú honlapokat. Ezek után pedig a tartalmakról tájékoztatnák a rendőrséget. Ugyanezen technikával kellene felderíteni azokat az „ügyfeleket” is, akik hitelkártyájuk igénybe vételével rendelnek „egyre szabott” gyermekpornográfiák vagy „snuff movie”-t⁽¹⁾. Szükség esetén a jogalkotónak kötelezővé kell tennie az ilyenfajta ellenőrzéseket. Az internetes keresőprogramokat is úgy kellene kialakítani, hogy az internetezők bizonyos kulcsszavak és -kifejezések segítségével csak nehezen bukkanhassanak rá gyermekpornót vagy más bűnös tartalmú szövegeket kínáló oldalakra.

3.13 Mindehhez az állami hatóságok részéről is történő hatékony fellépés alkalmas eszközeire, szakképzett állományra, általánosított, határokon átnyúló együttműködésre és nemzeti, európai és nemzetközi szinten összehangolt szabályozásra van szükség, amely nem sérti a hálózatra való kapcsolódást a világhálón, de lehetővé teszi az Internetet illegális tartalmak közvetítésére használó személyek és csoportok ártalmatlanítását, illetve a nem helyénvaló vagy káros tartalmak fogadásának önszántukból való megakadályozását.

3.14 Hogy hatékony legyen, ez a fellépés közvetlenül be kell, hogy vonja az összes Internet-használót, akiket képezni és tájékoztatni kell a szükséges óvintézkedésekről és azokról az eszközökről, amelyek segítségével megvédhetik magukat az

ilyen veszélyes vagy nem kívánatos tartalmak fogadásától, valamint attól, hogy ilyen tartalmak önhibájukon kívüli továbbításává váljanak. Az EGSZB szerint a terv képzési és tájékoztatási része mindenképp a felhasználók mozgósítására kell, hogy összpontosítson, hogy nagyobb felelősséggel viseltesenek maguk és felhasználóik iránt. Problémát jelentenek a szabályozatlan, egészséggel kapcsolatos webhelyek. A vállalatoknak is foglalkozniuk kell dolgozóik képzésével, valamint hálózataik és elektronikus kereskedelmet bonyolító webhelyeik biztonságosabbá tételével. A közigazgatási, köz- és magánintézményeknek úgyszintén alkalmazniuk kell ezeket a biztonsági intézkedéseket, és gondoskodniuk kell az általuk kezelt adatok, így különösen a személyes adatok abszolút bizalmas kezeléséről. A probléma további tudatosítása együtt kell, hogy járjon a minőségi on-line tartalmak előmozdításával, valamint a „hosszas” böngészés és az egyes esetekben személyiségtorzulást okozó szerepjátékok alternatívájaként megjelenő nem-internetes tevékenységekre történő ösztönzéssel.

3.15 Arra is szükség van, hogy a felhasználók rendelkezzenek olyan eszközökkel, melyek segítségével könnyen bejelenthetik az általuk a világhálón talált illegális tartalmakat telefonos ügyfélszolgálatoknak, elismert speciális segélykérő szervezeteknek vagy speciális rendőri egységeknek annak érdekében, hogy figyelemztessék a hatóságokat, és azok ha kell, megfelelő intézkedéseket tegyenek. Figyelmeztetni kellene a szülőket azokban az országokban, ahol gyakoriak az on-line vagy különböző adathordozókon hozzáférhető gyermekpornográfia céljából történő visszaélések, például az Unió határain kívül. Ezt bele lehetne ágyazni bizonyos külkapcsolati együttműködési programok (RELEX) keretében.

3.16 Az EGSZB amellett, hogy helyesli a program konkrét célkitűzéseit (a törvénytelen tartalmak bejelentésének lehetővé tétele forródróton keresztül, nem kívánt tartalmak szűrésére szolgáló technológiák fejlesztése, tartalmak osztályozása, küzdelem a spam ellen, az ágazat önszabályozása és a technológiák biztonságos használatának megismertetése), konkrét megjegyzéseiben néhány további cél kitzését javasolja, melyek véleménye szerint megfontolandónak tűnnek.

4. Az EGSZB külön megjegyzései

4.1 Az EGSZB a múltban már kérte az Európai Bizottságtól, hogy csökkenjen az EU által finanszírozott programok túlzott bürokratikusága, aminek legnagyobb előnye az lenne, hogy megkönnyítene a mikro-projektek, illetve a helyi szintű nem kormányzati szervezetek forrásokhoz juttatását. Az EGSZB hasznosnak látná az – elsősorban – a program keretében elért kézzelfogható eredményekre és a javasolt megoldások hatékonyságára irányuló ellenőrzés megvalósulását. A megoldások elterjesztését nem kellene annyira bizalmas módon kezelni.

4.2 Az EGSZB szerint meg kellene fontolni olyan szabályozási megoldásokat – ha lehetséges, akkor az itt tárgyalt program keretében, vagy ha nem, akkor az Európai Bizottság új kezdeményezése keretében –, amelyek támogatnák a végfelhasználók védelmét.

(1) Olyan filmek, amelyekben a bemutatott szélsőséges erőszak, kínzás és gyilkosságok valóságosak.

4.3 Az Internet-hozzáférést biztosító szoftverek, a kiszolgálók operációs rendszerei vagy a tűzfalprogramok szerzőinek teljes felelősséget kell viselniük termékeikért. A felhasználók számára garantálni kell, hogy ezek a szoftverkészítők a rendelkezésre álló legjobb technikákat használják és rendszeresen frissítik termékeiket. A felhasználók számára nyújtott garanciát erősíteni kell önszabályozással, illetve ennek híján közösségi normával.

4.4 Az Internet-szolgáltatóknak – ahogy ezt sokan közülük már most is teszik – könnyen kezelhető, a webhelyről elérhető vírusellenes eszközöket kell felkínálniuk az üzenetek vagy csatolt fájlok letöltése előtt, valamint előzetes szűrőket a spam ellen. Ez kereskedelmi előnyhöz juttathatja azokat a szolgáltatókat, akik komoly erőfeszítéseket tesznek fogyasztóik védelmében. Mivel a gyerekek az Internet-használat tekintetében gyakran szüleik előtt járnak, a levélszűrő, vírusirtó, tűzfalat és szülői ellenőrzést biztosító rendszereket előre kell telepíteni, és úgy kell őket kialakítani, hogy különösebb technikai ismeretek nélkül is könnyen kezelhetőek legyenek.

4.5 A programnak támogatnia kell a kutatást is a speciális szoftverek és más, annak megállapítására szolgáló eszközök terén, hogy e különböző biztonsági és védelmi célokot szolgáló szoftverek kódjai mennyire „feltörhetetlenek”. Egyben ösztönöznie, vagy szükség esetén köteleznie kellene a szolgáltatókat arra, hogy minden észlelt vagy jelentett hiba esetén, mely lehetővé teszi a bejutást, rövid időn belül javításokat (patch) küldjenek, valamint arra, hogy fejlesszék a tűzfal-hardvereket illetve -szoftvereket, csakúgy mint a szűrésre és a tartalom valós eredetének azonosítására szolgáló módszereket.

4.6 Az EGSZB szívesen vette volna a korábbi Safer Internet terv hatékonyságának és eredményeinek értékelését a projekt által érintett problémák szerinti csoportosításban, és ennek szélesebb körben való terjesztését. Biztosítani kell, hogy a finanszírozott programokhoz vezető hivatkozások aktívak maradjanak, és a felhasználók megismerjék ezeket. Az Európai Bizottság honlapjának is tájékoztatnia kellene a tagállamok vagy más országok által tett kezdeményezésekről és az általuk szerzett tapasztalatokról az ismeretek és a hasznosnak bizonyult tapasztalatok cseréje vagy az együttműködés érdekében.

4.7 Teljes mértékben lehetséges jogi lépéseket is tenni. Az Internet-szolgáltatók, a hitelkártyacégek és az internetes keresők mind szabályozhatók, sőt néhányan közülük már most is önszabályozásnak vetik alá magukat. A terrorizmust, rasszizmust, öngyilkosságot és gyermekpornográfiát hirdető webhelyek esetében szigorú és elrettentő hatású büntetőjogi következményeket kell kilátásba helyezni. Az eddigieknél jelentősebb nemzetközi együttműködésre van szükség az ilyen honlapok

felderítése és azonosítása, illetve – minden adódó lehetőséget kihasználva – ezek bezárása érdekében, de legalább is tárgyalásokat kell kezdeni ebből a célból a hasonló honlapoknak otthont adó országokkal.

5. Következtetések

Amellett, hogy támogatja a „Safer Internet plus” program folytatását és kiterjesztését, az EGSZB (amely egyébként e program létrehozását követelte) úgy véli, hogy a visszaélések általi fenyegetettség komolysága és mértéke – elsősorban a gyerekek esetében – sürgős kiegészítő jogalkotást és eseti, gyakorlati intézkedéseket tesz szükségessé a következő területeken:

- legyen minden érintett szereplő általános kötelezettsége, hogy védelmezze a gyermekeket és általában a felhasználókat, különösen a legvédtelenebbeket,
- szűrőrendszerek automatikus telepítése,
- világos biztonsági üzenetek minden internetes csevegőhelyet (chat room-ot) működtető honlapon és portálon,
- olyan egyesületek támogatása, amelyek közvetlen telefonvonalakat (forródrótot) hoznak létre a gyermekek számára súlyosan káros webhelyek és on-line tevékenységek bejelentésére,
- a hitelkártyák gyermekpornográfia vagy más illegális tartalom rendelkezésre való felhasználásának, illetve a piszkos pénzek kifizetésének megakadályozása,
- a szülők, a nevelők és a hatóságok figyelmeztetése azokban az országokban, ahol a gyermekpornográfiával összefüggő visszaélések aggasztó szintet értek el,
- több intézkedés a gyermekpornográfiával összefüggő visszaélések és a szervezett bűnözés közötti kapcsolatok ügyében,
- káros tartalmakat azonosító, azokról tájékoztató és a rasszista tartalmakat eltávolító rendszerek, tájékoztatás internetes csalási kísérletekről vagy egészségkárosító vegyületek árusításáról a kiszolgáltatók vagy nem eléggé tájékozott emberek védelmében.
- törekvés a nemzetközi együttműködésre és a közös szabályozásra a spam elleni hatékonyabb fellépés érdekében,
- nemzetközi együttműködés (a korai figyelmeztetés rendszerének javítása) és elrettentő hatású büntetőjogi szankciók alkalmazása az informatikai vírusok terjesztőivel és a magán- és közhálózatok bűnös célú (a hálózatba való betörés és annak elfoglalása ipari kémkedés, sávzsélesség lefoglalása és más visszaélések céljából), illetéktelen használatával szemben.

Brüsszel, 2004. december 16.

Az Európai Gazdasági és Szociális Bizottság

Elnöke

Anne-Marie SIGMUND